WHAT IS CLAIMED IS:

1. A method for encrypted data storage in a storage system:

converting encrypted blocks of data to produce corresponding converted blocks of data, wherein an encrypted block of data is encrypted with first cryptographic criteria, wherein a converted block of data is encrypted with second cryptographic criteria;

receiving a read request during said step of converting in order to access read data from said storage system and in response thereto accessing said read data from at least one decrypted block of data, wherein if said read data is stored in an encrypted block of data, then decrypting it using said first cryptographic criteria to produce said at least one decrypted block of data, wherein if said read data is stored in a converted block of data, then decrypting it using said second cryptographic criteria to produce said at least one decrypted block of data; and

receiving a write request during said step of converting in order to store write data to said storage system and in response thereto writing at least a first block of data to said storage system, said first block of data comprising data to be written, wherein if said first block of data is targeted to an encrypted block of data, then encrypting at least some of it using said first cryptographic criteria to produce said first block of data, wherein if said first block of data is targeted to a converted block of data, then encrypting at least some of it using said second cryptographic criteria to produce said first block of data.

2. The method of claim 1 wherein said step of converting comprises a step of replacing each encrypted block of data by its corresponding converted block of data.

3. The method of claim 1 wherein some of said steps of encrypting and decrypting comprise executing computer program code on a data processing component.

4. The method of claim 3 further comprising accessing at least one of said encryption and decryption criteria over a communication network.

5. The method of claim 1 wherein some of said steps of encrypting and decrypting are performed on logic circuitry configured to perform cryptographic operations.

6. The method of claim 1 wherein said read request is a file-level read request and said step of accessing said read data includes producing one or more block-level read requests based on said file-level read request.

7. The method of claim 6 wherein said write request is a file-level write request and said step of writing at least a first block of data includes producing one or more block-level write requests based on said file-level write request.

8. The method of claim 7 wherein said file-level read request and said file-level write request are received from a host device.

9. A method for storing encrypted data on a storage system comprising:

converting first data blocks of said storage system to produce corresponding second data blocks, including encrypting said first data blocks to produce said second data blocks and replacing each first data block with its corresponding second data block; and

accessing read data from said storage device in response to a read request, including accessing a third data block and decrypting said third data block if said third data block is one of said second data blocks, to produce a decrypted data block so that said read data can be read therefrom,

wherein said step of accessing read data is performed during said step of converting so that said converting does not prevent read access to said storage system.

10. The method of claim 9 further comprising storing a fourth data block to said storage device in response to a write request, said fourth data block comprising data to be written, said step of storing including encrypting said fourth data block if it is to be written to one of said second data blocks, wherein said step of storing is performed during said step of converting so that said converting does not prevent write access to said storage system.

11. The method of claim 9 wherein said first data blocks are not encrypted.

12. The method of claim 9 wherein said first data blocks are encrypted with first encryption criteria and said second data blocks are encrypted with second encryption criteria, the method further comprising, prior to said step of encrypting first data blocks, a step of applying first decryption criteria to said first data blocks to decrypt said first data blocks.

13. The method of claim 12 wherein said step of decrypting said third data block includes applying first decryption criteria to said third data block if said third data block belongs to one of said first data blocks and applying second decryption criteria to said

third data block if said third data block belongs to one of said second data blocks, to produce said decrypted data block.

14. The method of claim 13 further comprising storing a fourth data block to said storage device in response to a write request, said fourth data block comprising data to be written, said step of storing comprising:

encrypting said fourth data block with said first encryption criteria if it is to be written to one of said first data blocks; and

encrypting said fourth data block with said second encryption criteria if it is to be written to one of said second data blocks,

wherein said step of storing is performed during said step of converting so that said converting does not prevent write access to said storage system.

15. A storage system comprising:

a storage component; and

a cryptographic component in data communication with said storage component and operable to convert unconverted blocks of data stored thereon to produce corresponding converted blocks of data, each converted block of data replacing its corresponding unconverted block of data on said storage component and in the same location as its corresponding unconverted block,

wherein said cryptographic component is further operable to receive read and write requests for data stored on said storage component, while unconverted blocks of data are converted to converted blocks of data,

wherein said cryptographic component is further operable to process a read request by accessing read blocks associated with said read request from said storage component, wherein if a read block is unconverted, then performing a first cryptographic process on said read block to produce an unencrypted read block, wherein if said read block is converted, then performing a second cryptographic process on said read block to produce said unencrypted read block,

wherein said cryptographic component is further operable to process a write request by writing one or more write blocks associated with said write request from said storage component, wherein if a write block is to be written to a block location that contains an unconverted block, then performing said first cryptographic process on said write block prior to writing said write block, wherein if a write block is to be written to a block location

that contains a converted block, then performing said second cryptographic process on said write block prior to writing said write block.

16. The storage apparatus of claim 15 further comprising a file system component configured to receive file-level read and write requests from one or more host devices, to produce said read and write requests based on said file-level read and write requests, and to communicate said read and write requests to said cryptographic component.

17. The storage apparatus of claim 15 wherein said storage component comprises an I/O interface and said cryptographic component comprises a first I/O interface and a second I/O interface, wherein said first I/O interface is configured for communication with a host device, wherein said second I/O interface is in data communication with said I/O interface of said storage component.

18. The storage apparatus of claim 15 wherein said cryptographic component comprises one or more encryption engines.

19. The storage apparatus of claim 15 wherein said cryptographic component is further operable to obtain criteria which specify said second cryptographic process prior to converting unconverted blocks of data to converted blocks of data.

20. The storage process of claim 15 wherein said first cryptographic process is a NULL process.

21. A method for storing and accessing data on a storage system comprising:

receiving from a host device file-level I/O requests;

converting blocks of data stored in said storage system, including for each block of data:

performing a first decryption of said block of data to produce an unencrypted block of data, said block of data being encrypted by a first encryption;

performing a second encryption of said unencrypted block of data to produce an encrypted block of data; and

overwriting said block of data;

during said converting, receiving and servicing a file-level read request; and

during said converting, receiving and servicing a file-level write request,

wherein servicing said file-level read request comprises:

producing one or more block-level read operations; and

decrypting a corresponding block of said block-level read operation with either said first or second decryption depending on how it was encrypted,

wherein servicing said file-level write request comprises:

producing one or more block-level write operations;

encrypting a corresponding block of data of said block-level write operation with said first encryption, if it is targeted to a block location in said storage system containing data that was encrypted with said first encryption; and

encrypting said corresponding block of data of said block-level write operation with said second encryption, if it is targeted to a block location in said storage system containing data that was encrypted with said second encryption.

22. The method of claim 21 wherein some of said steps of encrypting and decrypting comprise executing computer program code on a data processing component.

23. The method of claim 22 further comprising accessing at least one of said encryption and decryption criteria over a communication network.

24. The method of claim 21 wherein some of said steps of encrypting and decrypting are performed on logic circuitry configured to perform cryptographic operations.

25. The method of claim 21 wherein said blocks of data are converted in sequential order as they are stored in said storage system.

26. The method of claim 21 further comprising receiving information identifying a list of blocks to be converted.